Stallings Graphs, Algebraic Extensions and Primitive Elements in $\mathbf{F}_2$

Ori Parzanchevski[†] and Doron Puder[‡]

October 25, 2012

Abstract

This paper studies the free group of rank two from the point of view of Stallings core graphs. The first half of the paper examines primitive elements in this group, giving new and self-contained proofs for various known results about them. In particular, this includes the classification of bases of this group. The second half of the paper is devoted to constructing a counterexample to a conjecture by Miasnikov, Ventura and Weil, which seeks to characterize algebraic extensions in free groups in terms of Stallings graphs.

1 Introduction

Let $\mathbf{F}$ be a finitely generated free group. A subgroup J of $\mathbf{F}$ is said to be an *algebraic extension* of another subgroup H, if $H \leq J$ and there does not exist an intermediate subgroup $H \leq M \lneq J$ such that M is a proper free factor of J. We denote this by $H \leq_{alg} J$. This notion, which was formulated independently by several authors (and already appears in [Tak51]), is central to the understanding of the lattice of subgroups of $\mathbf{F}$. For example, it can be shown that every extension $H \leq J$ of free groups admits a unique intermediate subgroup $H \leq_{alg} M \leq_{ff} J$ (where $\leq_{ff}$ denotes a free factor). Moreover, if $H \leq \mathbf{F}$ is a finitely generated subgroup, it has only finitely many algebraic extensions in $\mathbf{F}$. Thus, every group containing H is a free extension of one of the algebraic extensions of H, which is a well known theorem of Takahasi [Tak51]. For proofs of the mentioned facts, as well as a general survey of algebraic extensions, we refer the reader to [MVW07]. $H \leq_{alg} J$

Given a basis X of $\mathbf{F}$ and $H \leq \mathbf{F}$, we denote by $\Gamma_X(H)$ the *Stallings core graph* of H with respect to X. This is a pointed, directed, X-labeled graph, such that the words formed by closed paths around the basepoint are precisely the elements of H, and which is minimal with respect to this property. One way to construct this graph is by taking the Schreier right coset graph of H in $\mathbf{F}$ w.r.t. X and then deleting all "hanging trees", i.e., all $\Gamma_X(H)$

[†]Supported by an Advanced ERC Grant. [‡]Supported by the Adams Fellowship Program of the Israel Academy of Sciences and Humanities.

edges which are not traced by some non-backtracking loop around the basepoint. Figure 1 demonstrates the core graph of $H = \langle ab^{-1}a, a^{-2}b \rangle$ for $X = \{a, b\}$ and $\mathbf{F} = \mathbf{F}(X)$. We refer to [Sta83, KM02, MVW07, Pud11] for further background on Stallings graphs.

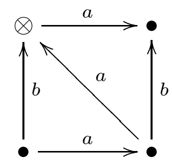


Figure 1: The core graph $\Gamma_X(H)$ where $X = \{a, b\}$ and $H = \langle ab^{-1}a, a^{-2}b \rangle \le \mathbf{F}(X)$.

Given the basis X, and two subgroups $H, J \le \mathbf{F}$, there is a graph morphism (which preserves the basepoint, directions and labeling) from $\Gamma_X(H)$ to $\Gamma_X(J)$ if and only if $H \le J$. Such a morphism is unique, when it exists. Given $H, J \le \mathbf{F}$, we say that H X*-covers* J if $H \le J$ and the morphism from $\Gamma_X(H)$ to $\Gamma_X(J)$ is onto. We denote this by $H \le_{\overrightarrow{X}} J$. (In [MVW07] this is indicated by saying that J is a "X-principal overgroup" of H, and by the notation $J \in \mathcal{O}_X(H)$.) X*-covers* $\le_{\overrightarrow{X}}$

It is not hard to see (e.g. [MVW07, prop. 3.7], or [PP12, claim 3.2]) that if $H \le_{alg} J$, then $H \le_{\overrightarrow{X}} J$ for every basis X of $\mathbf{F}$. The following conjecture, raised in [MVW07], asks whether the converse also holds.

Conjecture ([MVW07, §5(1)])**.** *If $H \le J \le \mathbf{F}$ and $H \le_{\overrightarrow{X}} J$ for every basis X of $\mathbf{F}$ then J is an algebraic extension of H.*

The main result of this paper is a counterexample to this conjecture:

Proposition (Prop. 4.1)**.** *Let $\mathbf{F}_2 = \mathbf{F}(a, b)$ be the free group on two generators, $H = \langle a^2b^2 \rangle$, and $J = \langle a^2b^2, ab \rangle$. Then $H \le_{\overrightarrow{X}} J$ for every basis X of $\mathbf{F}_2$, but J is not an algebraic extension of H.*

The relation "$H \le_{\overrightarrow{X}} J$" is basis-dependent, while the relation "$H \le_{\overrightarrow{X}} J$ for every basis X" is intrinsic, as is "$H \le_{alg} J$". Proposition 4.1 means that the latter two relations are different, and this raises the intriguing question of understanding the algebraic significance of "covering with respect to all bases".

The proof of Proposition 4.1 follows from a thorough analysis of Stallings graphs, using classical results (e.g. [Nie17, Coh72, CMZ81, OZ81]) on primitive elements and bases of $\mathbf{F}_2$. It turns out that these results can also be proven by appealing solely to Stallings graphs, and we use the opportunity to provide self-contained proofs for them in Section 3. Section 2 recalls some basic facts about Stallings graphs and foldings, and presents two auxiliary lemmas which will be used later on. Finally, the proof of the counterexample (Proposition 4.1) is given in Section 4, and some concluding remarks in Section 5.

2 Stallings Graphs

We assume that the reader is familiar with the theory of Stallings foldings, but recall the basic facts. If Γ is a pointed, directed, X-labeled graph, we denote by $\pi_1^X(\Gamma)$ the $\pi_1^X(\Gamma)$

subgroup of $\mathbf{F} = \mathbf{F}(X)$ consisting of the words which appear as closed loops around the basepoint of Γ. The operators π_1^X and Γ_X constitute a bijection between subgroups of $\mathbf{F}(X)$ and X-labeled core graphs, which matches f.g. subgroups to finite graphs.

If Γ is a finite (pointed, directed) X-labeled graph, and $\pi_1^X(\Gamma) = H$, then $\Gamma_X(H)$ is obtained from Γ by repeatedly performing one of the following operations, in any order, until neither of them is possible:

(1) *Folding* - merging two edges with the same label, and the same origin or terminus (and thus merging also the other ends).

(2) *Trimming* - deleting a leaf which is not the basepoint, and the edge which leads to it.

The following lemma shows that under certain conditions only foldings are necessary in this process:

Lemma 2.1. *Let Γ be a finite, pointed, directed, X-labeled graph such that at every vertex, except possibly the basepoint, there are at least two types of edges (the type of an edge consists of its label and direction). Then the core graph $\Gamma_X(H)$ of $H = \pi_1^X(\Gamma)$ is obtained from Γ by foldings alone (i.e. without trimming).*

Proof. Evidently, Γ cannot have leaves, except for possibly the basepoint. Folding steps do not decrease the number of types of edges at a vertex, so that the property in the statement still holds after every folding step, and no new leaves are created throughout the process. $\square$

This simple lemma will prove out to be extremely useful. It already plays a role in Lemma 2.3, which characterizes X-covering in simple extensions.

Definition 2.2. Let Γ be a pointed and directed X-labeled graph and let $w \in \mathbf{F}$. We say that w *appears in* Γ if there exist paths p_1, p_2 in Γ such that p_1 starts at the basepoint, p_2 terminates at the basepoint, and $w = p_1 p_2$ (i.e. $p_1 p_2$ is the presentation of w as a reduced word in $X \bigcup X^{-1}$). *appears in*

For example, for H in Figure 1, a^3 and a^2ba^{-1} appear in $\Gamma_X(H)$, but a^2b^2 does not. Notice that if w appears in Γ, s.t. $\pi_1^X(\Gamma) = H$, and Γ satisfies the conditions of Lemma 2.1, then w appears in $\Gamma_X(H)$ as well. This will play a significant part in Section 4.

Lemma 2.3. *Let $H \leq \mathbf{F}$, $w \in \mathbf{F}$ and $J = \langle H, w \rangle$. Then $H \leq_{\vec{X}} J$ iff w appears in $\Gamma_X(H)$.*

Proof. Assume first that w appears in $\Gamma_X(H)$, and let p_1, p_2 be as in Definition 2.2. Denote by Γ the graph obtained from $\Gamma_X(H)$ by identification of p_1's endpoint and p_2's start-point. We have $\pi_1^X(\Gamma) = J$, and the (pointed, directed, labeled) map from $\Gamma_X(H)$ to Γ is onto. Since Γ satisfies the conditions of Lemma 2.1, $\Gamma_X(J)$ is obtained from it by foldings alone. We have now that $\Gamma_X(H)$ maps onto Γ, which maps onto $\Gamma_X(J)$, and by transitivity it follows that $H \leq_{\vec{X}} J$.

Assume now that w does not appear in $\Gamma_X(H)$. Let p_1 be the maximal path beginning at the basepoint of $\Gamma_X(H)$ which is a prefix of w, and denote by v_1 its endpoint. Let p_2 be the maximal path ending at the basepoint of $\Gamma_X(H)$ which is a suffix of w, and v_2 its beginning. If $w = p_1 w' p_2$, take $\Gamma = \Gamma_X(H) \bigcup p_{w'}$ where $p_{w'}$ is a path labeled by w', whose beginning is attached to v_1, and whose endpoint to v_2 (see Figure 2). Now $\pi_1^X(\Gamma) = J$ and Γ has no foldable edges nor leaves, i.e. $\Gamma = \Gamma_X(J)$. Thus $\Gamma_X(H)$ is a subgraph of $\Gamma_X(J)$, and in particular does not map onto it. (In fact, since the map from $\Gamma_X(H)$ to $\Gamma_X(J)$ is injective, H is a free factor of J.)

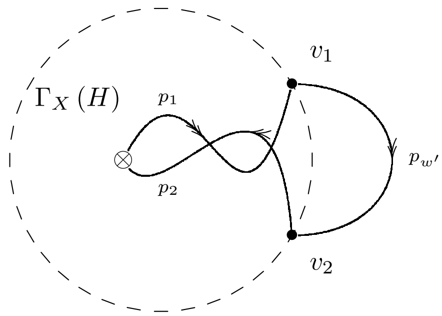


Figure 2: $\Gamma = \Gamma_X(H) \bigcup p_{w'}$

$\square$

Remark 2.4. With some further work, the basic idea of Lemma 2.3 can lead to an algorithm to detect primitive words and free factors in $\mathbf{F}$. See [Pud11, Thm 1].

3 Primitives in $\mathbf{F}_2$

In this section we give new proofs for the classical theorems on primitive words and bases of $\mathbf{F}_2$ [Nie17, Coh72, CMZ81, OZ81]. Throughout the section X denotes the basis $\{a, b\}$ of $\mathbf{F}_2 = \mathbf{F}(a, b)$.

We start with the following lemma, which reduces the classification of bases of $\mathbf{F}_2$ to that of cyclically reduced (henceforth: CR) bases. *CR*

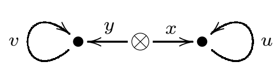
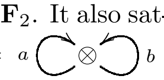
Lemma 3.1. *Let $Y = \{\overline{u}, \overline{v}\}$ be any basis of $\mathbf{F}_2$.*

(1) Write $\overline{u} = xux^{-1}$ † and $\overline{v} = yvy^{-1}$ with u, v CR. Then either x is a prefix of y or y is a prefix of x.

(2) Assume that x is a prefix of y, and write $\overline{u} = xux^{-1}$ and $\overline{v} = xwvw^{-1}x^{-1}$. Then w is a prefix of some power of u or of u^{-1} (which implies that $w^{-1}uw$ is a cyclic rotation of u).

(3) The basis $(xw)^{-1} Y xw = \{w^{-1}uw, v\}$ is CR.

Therefore, any basis of $\mathbf{F}_2$ is of the form $\{xux^{-1}, xwvw^{-1}x^{-1}\}$ where w is a prefix of some power of $u^{\pm 1}$, $\{w^{-1}uw, v\}$ is a CR basis, and x is any word s.t. xux^{-1} and $xwvw^{-1}x^{-1}$ are reduced.

Proof. The graph $\Gamma =$  satisfies $\pi_1^X(\Gamma) = \langle \overline{u}, \overline{v} \rangle = \mathbf{F}_2$. It also satisfies the conditions of Lemma 2.1, and must therefore fold into $\Gamma_X(\mathbf{F}_2) =$  .

† By "write" we mean that xux^{-1} is a reduced expression of $\overline{u}$ - no cancellation is needed. This convention will repeat throughout the paper, and we will not mention it again.

The only vertex at which folding may occur is the basepoint $\otimes$, and after the first identification of edges the only possible folding place is at the identified termini. Continuing in this manner shows that for Γ to fold into $\Gamma_X(\mathbf{F}_2)$, the shorter word among x, y must be completely merged with a prefix of the longer one, giving (1). By the same arguments, the graph $\Gamma' = v \circlearrowright \bullet \xleftarrow{w} \otimes \circlearrowleft u$ must fold into $\Gamma_X(\mathbf{F}_2)$, and for this to happen w must wind itself completely around u, or around u^{-1} (i.e. w must be a prefix of some power of u or of u^{-1}). It follows that $w^{-1}uw$ is a cyclic rotation of u, and $\{w^{-1}uw, v\}$ is a CR basis. $\square$

Moving on to CR bases, we have the following:

Proposition 3.2. *Let $\{u, v\}$ be a CR basis of $\mathbf{F}_2$, such that $|u| + |v| \geq 3$* † *, and $|u| \leq |v|$. Then either u is a prefix or a suffix of v, or u^{-1} is.*

Proof. Since $|v| \geq 2$ and v is not a proper power, v contains both a and b, and thus $\langle v \rangle \leq_{\overrightarrow{X}} \mathbf{F}_2$. Since $\mathbf{F}_2 = \langle u, v \rangle$, Lemma 2.3 implies that u appears in $\Gamma_X(\langle v \rangle)$, which is just a cycle labeled by v as a word in $X \cup X^{-1}$.

Let p' be the maximal prefix of u which is a path emanating from the basepoint of $\Gamma_X(\langle v \rangle)$. Since $|u| \leq |v|$, this means that p' is a prefix of v or of v^{-1}. By inverting v if necessary we assume that p' is a prefix of v. Let s' be the maximal suffix of u which is a path ending at the basepoint of $\Gamma_X(\langle v \rangle)$. Since u is CR, s' cannot be a suffix of v^{-1}, and must be a suffix of v.

Let m be the middle part of u where p' and s' overlap (it may be empty: $|m| = |p'| + |s'| - |u| \geq 0$). Write $p' = pm$, $s' = ms$, which means that $u = pms$ (see Figure 3). Thus, if p is empty then $u = pms = s'$ is a suffix of v, and if s is empty then u is a prefix of v. We proceed to show that they cannot be both nonempty.

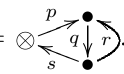
Figure 3: Illustration of the decomposition of v.

<table>
<tr><td colspan="10">v</td></tr>
<tr><td colspan="7">p'</td><td colspan="3"></td></tr>
<tr><td colspan="3"></td><td colspan="7">s'</td></tr>
<tr><td>p</td><td colspan="2">t</td><td colspan="6">m</td><td>s</td></tr>
<tr><td>p</td><td colspan="6">m</td><td colspan="2"></td><td>s</td></tr>
<tr><td>p</td><td>q</td><td>r</td><td>q</td><td>r</td><td>$\dots$</td><td>q</td><td>r</td><td>q</td><td>s</td></tr>
</table>

Let $\Gamma = u \circlearrowright \otimes \circlearrowleft v$. Since $\pi_1^X(\Gamma) = \langle u, v \rangle = \mathbf{F}_2$ and Γ satisfies the conditions of Lemma 2.1, it must fold into $\Gamma_X(\mathbf{F}_2) = a \circlearrowright \otimes \circlearrowleft b$, and we will show that this cannot happen if $p, s \neq 1$.

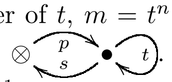
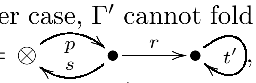
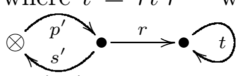
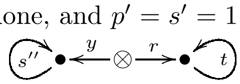
Assume therefore that $p, s \neq 1$. Since $|v| \geq |u|$ we can write $v = ptms$, and $t \neq 1$ since otherwise $u = v$ (this shows, in particular, that $|v| > |u|$). Since pm is a prefix of v, m is a prefix of tm, which means that m is a prefix of some (positive) power of t (see again Figure 3). We consider two cases:

† Here $|w|$ is the length of w as a reduced word in $X \cup X^{-1}$.

Case (i): m is not a power of t. In this case $t = qr$ with $q, r \neq 1$, and $m = (qr)^n q$ with $n \geq 0$ (see Figure 3; $n = 0$ corresponds to the possibility that p' and s' do not overlap in v). Since $u = p\,(qr)^n\, qs$ and $v = p\,(qr)^{n+1}\, qs$, Γ folds into $\Gamma' =$ .

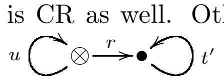
We aim to show that no folding can occur in Γ', but let us first introduce the following notations: for $w \in \mathbf{F}(X)$, we denote by w_1 the first letter of w as a reduced word in $X \cup X^{-1}$, and for two words w, w' we write $w \perp w'$ to indicate that $w_1 \neq (w')_1$. Namely, $w \perp w'$ implies that no folding occurs in $\xleftarrow{w} \bullet \xrightarrow{w'}$. $\perp$

Returning to Γ', we have $p \perp s^{-1}$ since u (or equivalently v) is CR, so no folding occurs at $\otimes$. Since $v = p\,(qr)^{n+1}\, qs$ is reduced, $p^{-1}, r^{-1} \perp q$ and $q^{-1} \perp r, s$. We also have $r \perp s$, for otherwise $p's_1 = p\,(qr)^n\, qr_1$ would be a common prefix of $u = p's$ and $v = p\,(qr)^{n+1}\, qs$, contradicting the maximality of p'. Finally, $r^{-1} \perp p^{-1}$ follows in the same way from the maximality of s', and we conclude that Γ' cannot be folded any further, i.e. $\Gamma' = \Gamma_X(\langle u, v\rangle)$, which contradicts $\Gamma_X(\langle u, v\rangle) = \Gamma_X(\mathbf{F}_2)$.

Case (ii): m equals a power of t, $m = t^n$ $(n \geq 0)$, so that $u = pt^n s$ and $v = pt^{n+1}s$. This time Γ folds into $\Gamma' =$ . We have $p \perp s^{-1}$ as before; $p^{-1} \perp t$ and $t^{-1} \perp s$ follows from $v = pt^{n+1}s$ being reduced; $s \perp t$ holds, since otherwise $pt^n s_1 = pt^n t_1$ would be a common prefix of u and v, contradicting the maximality of $p' = pt^n$; likewise, $p^{-1} \perp t^{-1}$ by the maximality of s'. Now, if $n > 0$ then $t \perp t^{-1}$ since $v = pt^{n+1}s$ is reduced, and if $n = 0$ then $p^{-1} \perp s$ since $u = ps$ is reduced. In either case, Γ' cannot fold into $\Gamma_X(\mathbf{F}_2)$: For $n = 0$, assuming that Γ' folds at all, $\Gamma_X(\langle u, v\rangle) =$ , where $t = rt'r^{-1}$ with t' CR. Thus, $\Gamma_X(\langle u, v\rangle) \neq \Gamma_X(\mathbf{F}_2)$. For $n > 0$, Γ' folds into  where r is the common suffix of p and s^{-1}, so that $p = p'r$, $s = s'r$. If $p', s' \neq 1$ we are done, and $p' = s' = 1$ is impossible since $p \perp s^{-1}$. If $p' = 1 \neq s'$ then the graph folds into  where s'' is CR and $s' = ys''y^{-1}$, and likewise for $p' \neq 1 = s'$. $\square$

Definition. A word $w \in \mathbf{F}(a, b)$ is *monotone* if for every letter (a or b) all the exponents *monotone*
of this letter in w have the same sign.

Proposition 3.3. *A CR primitive word in* $\mathbf{F}_2$ *is monotone.*

Proof. Let u be a CR primitive. By Lemma 3.1, possibly applying some cyclic rotation to u, we can complete it to a CR basis $\{u, v\}$. We show that both u and v are monotone, by induction on $|u| + |v|$. The base case $|u| + |v| = 2$ is trivial. Assume that $|u| \leq |v|$. Using Proposition 3.2, and perhaps replacing u, v, or both of them by their inverses (which does not affect monotonicity), we can write $v = ut$. Now $\{u, t\}$ is a basis with $|u| + |t| < |u| + |v|$, and we claim that t is CR as well. Otherwise, $t = rt'r^{-1}$ with t' CR and $r \neq 1$, and we have $\Gamma_X(\langle u, t\rangle) =$ , as $u \perp u^{-1}$ since u is CR, $(t')^{-1} \perp t'$ since t' is, and all other relevant pairs since $v = urt'r^{-1}$ is. This, of course, contradicts $\langle u, t\rangle = \mathbf{F}_2$.

Therefore, by the induction hypothesis u and t are monotone. Assume first that $|u| \leq |t|$. Since $v = ut$ is CR, u^{-1} cannot be neither a prefix nor a suffix of t. Thus, by Proposition

3.2 u must be a prefix or a suffix of t, and in either case v is monotone. The same argument applies to the case $|u| > |t|$. $\square$

We stress the following observation made in the proof:

Corollary 3.4. *Let $\{u, v\}$ be a CR basis of $\mathbf{F}_2$ with u a prefix of v, and write $v = ut$. Then $\{u, t\}$ is again a CR basis.*

This leads to a constructive description of all CR bases of $\mathbf{F}_2$:

Proposition 3.5. *Any CR basis of $\mathbf{F}_2$ is obtained as follows: given a pair of positive co-prime integers (p, q), there is a unique sequence of pairs*

$$(p, q) = (p_0, q_0), (p_1, q_1), \ldots, (p_\ell, q_\ell) = (1, 1) \tag{3.1}$$

which is the result of applying the Euclidean g.c.d. algorithm (i.e. if $p_i < q_i$ then $p_{i+1} = p_i$ and $q_{i+1} = q_i - p_i$, and vice-versa). Let $X_\ell = \{u_\ell, v_\ell\}$ be one of the four bases $\left\{a^{\pm 1}, b^{\pm 1}\right\}$, and define $X_i = \{u_i, v_i\}$ iteratively for $i = \ell - 1 \ldots 0$ by

$$(u_i, v_i) = \begin{cases} (u_{i+1} \quad , \; v_{i+1} u_{i+1}) & p_i < q_i \\ (u_{i+1} v_{i+1} \, , \; v_{i+1} \quad) & q_i < p_i. \end{cases} \tag{3.2}$$

Finally, take X_0, conjugate its elements by any common prefix or suffix (thus cyclically rotating both of them), and possibly replace one of them by its inverse.

Proof. This construction certainly gives a CR basis of $\mathbf{F}_2$ (CR follows from monotonicity), and it remains to show that every CR basis is thus obtained. This is done by reversing the process, as follows. Let $\{x_0, y_0\}$ be a CR basis. Discarding the trivial bases $\left\{a^{\pm 1}, b^{\pm 1}\right\}$, we can assume (by inversion if necessary) that one of x_0 or y_0 is a prefix/suffix of the other (by Proposition 3.2).

Lemma. *x_0, y_0 can be rotated by a a common prefix/suffix, so that a sequence of CR bases $\{x_1, y_1\}, \ldots, \{x_\ell, y_\ell\}$ with the following properties is obtained:*

(1) For every $0 \le i \le \ell - 1$, the shorter of x_i, y_i is a suffix of the longer one.

(2) Each basis is obtained from the previous one by

$$(x_{i+1}, y_{i+1}) = \begin{cases} (x_i, t) & |x_i| < |y_i| \text{ and } y_i = t x_i \\ (t, y_i) & |y_i| < |x_i| \text{ and } x_i = t y_i. \end{cases} \tag{3.3}$$

(3) $\{x_\ell, y_\ell\}$ is one of the four bases $\left\{a^{\pm 1}, b^{\pm 1}\right\}$.

Proof of the Lemma. If we do not perform the rotation of x_0, y_0 by a common prefix/suffix, the same holds, but with the exception that at each stage the shorter among x_i, y_i may be a prefix of the longer one, and not a suffix: this follows from by Proposition 3.2, and Corollary 3.4, which ensures that all of these bases are CR. Assume that the

process first fails at step m, i.e. the shorter among x_m, y_m is not a suffix of the longer one, and assume for simplicity that x_m is shorter, so that $y_m = x_m t$.

Since x_0, y_0 are products of positive powers of x_m and $y_m = x_m t$, it follows that x_m is a common prefix of both of them. Therefore, $\{x'_0, y'_0\} = \left\{x_m^{-1} x_0 x_m, x_m^{-1} y_0 x_m\right\}$ is a cyclic rotation of $\{x_0, y_0\}$. Let $\{x'_i, y'_i\}_{i=0\ldots m}$ be the bases obtained by (3.3) from $\{x'_0, y'_0\}$. Since the expression of x'_i, y'_i as words in x'_m, y'_m is the same as that of x_i, y_i as words in x_m, y_m, we still have that at every step until m the shorter of x'_i, y'_i is a suffix of the longer one. In fact, $x'_i = x_m^{-1} x_i x_m$ and likewise for y'_i, for all $i \leq m$. Now, assertion *(1)* holds for step m as well, as $x'_m = x_m$ and $y'_m = x_m^{-1} (x_m t) x_m = t x_m = t x'_m$.

We continue in this manner: at the next step at which assertion *(1)* fails we replace $\{x'_0, y'_0\}$ by $\{x''_0, y''_0\}$ which resolves that step, and note that x''_0, y''_0 is still a cyclic rotation of the original x_0, y_0 by a common prefix/suffix, and that no new failures of *(1)* were introduced by this change for the previous steps. Repeating this for every failure of *(1)* guarantees that it hold throughout the process. $\square$

We continue the proof of the proposition, assuming that x_0, y_0 were inverted and rotated according to the Lemma, and $\{x_1, y_1\}, \ldots, \{x_\ell, y_\ell\}$ are the bases obtained by (3.3). The sequence of integer pairs $(|x_0|, |y_0|), \ldots, (|x_\ell|, |y_\ell|) = (1, 1)$ is then the sequence obtained by the Euclidean algorithm for $(|x_0|, |y_0|)$ (as in (3.1)), and in particular this shows that $|x_0|, |y_0|$ are co-prime. Thus, if one takes $(p, q) = (|x_0|, |y_0|)$ and $(u_\ell, v_\ell) = (x_\ell, y_\ell)$, and follows (3.2) as explained in the statement of the proposition, the process in (3.3) is reversed, and one obtains $(u_0, v_0) = (x_0, y_0)$. $\square$

Corollary 3.6. *For a CR basis $\{u, v\}$, regard u and v as cyclic words, and assume (by inverting u if necessary) that one of them is a subword of the other. Then one of a, b always appears (in both u and v) with exponent ε for some fixed $\varepsilon \in \{1, -1\}$, and the other letter always appears with exponent m or $m+1$ for some $m \in \mathbb{Z}$.*

Proof. Let $X_i = \{u_i, v_i\}$ $(0 \leq i \leq \ell)$ be the bases constructed in Proposition 3.5 to give $X_0 = \{u, v\}$. Assume, for simplicity, that $X_\ell = \{u_\ell, v_\ell\} = \{a, b\}$, and that in the first step the first option in (3.2) holds, so that $X_{\ell-1} = \{a, ba\}$. Let r be the number of times the first option in (3.2) holds before it fails, i.e. $X_{\ell-2} = \left\{a, ba^2\right\}, \ldots, X_{\ell-r} = \{a, ba^r\}$ (possibly $r = 1$). If $r = \ell$ then the statement holds. Otherwise, $X_{\ell-r-1} = \{aba^r, ba^r\}$, and now every cyclic word which is a product of the elements of $X_{\ell-r-1}$ (with positive exponents only) clearly satisfies the statement of the corollary with $\varepsilon = 1$ and $m = r$. Since u and v are such words, we are done. $\square$

4 The counterexample

Let $X = \{a, b\}$ and $\mathbf{F}_2 = \mathbf{F}(X)$. In this section we prove the following:

Proposition 4.1. *Let $H = \left\langle a^2 b^2 \right\rangle$, and $J = \left\langle a^2 b^2, ab \right\rangle$. Then $H \leq_{\overrightarrow{Y}} J$ for every basis Y of $\mathbf{F}_2$, but J is not an algebraic extension of H.*

Proof. First, as H is a free factor of J (since $J = H * \langle ab \rangle$), it is clear that J is not an algebraic extension of H, and it is left to show that H covers J with respect to every basis $Y = \{u, v\}$. For any automorphism φ of $\mathbf{F}_2$, $H \leq_{\vec{X}} J$ iff $\varphi(H)$ covers $\varphi(J)$ w.r.t. the basis $\varphi(X) = \{\varphi(a), \varphi(b)\}$. As $\varphi(X)$ achieves all bases of $\mathbf{F}_2$, what we seek to show is equivalent to the assertion that $\langle u^2v^2 \rangle \leq_{\vec{X}} \langle u^2v^2, uv \rangle$ for every basis $\{u, v\}$.

By Lemma 2.3, showing that $\langle u^2v^2 \rangle$ X-covers $\langle u^2v^2, uv \rangle$ is equivalent to verifying that uv appears in $\Gamma_X(\langle u^2v^2 \rangle)$. For the case where u and v are CR this is shown in Lemma 4.3, and the case where only one of them is CR is handled in Lemma 4.4. For the general case, let $Y = \{\overline{u}, \overline{v}\}$ be the base at hand, and write $\overline{u} = xux^{-1}$ and $\overline{v} = yvy^{-1}$ with u, v CR. By Lemma 3.1, x is a prefix of y, or vice-versa. Thus, if w is the shorter among x, y then $w^{-1}Yw$ is a basis with one CR element, which was already handled. Inferring from this the result for the original Y is done in Lemma 4.2. For this we need an additional technical assumption on $\Gamma_X(\langle w^{-1}\overline{u}^2\overline{v}^2 w \rangle)$, which is seen to hold in Lemmas 4.3 and 4.4. ◻

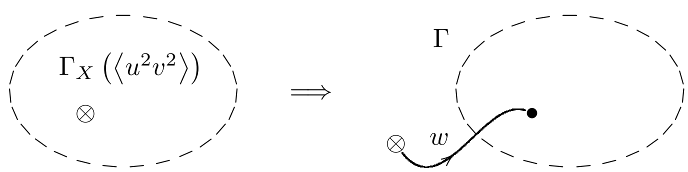
Lemma 4.2. *Let $\{\overline{u}, \overline{v}\}$ be a basis of $\mathbf{F}_2$ such that $\overline{u}$ and $\overline{v}$ share a common prefix w and a common suffix w^{-1}, and write $\overline{u} = wuw^{-1}$ and $\overline{v} = wvw^{-1}$. If*

(1) uv appears in $\Gamma_X(\langle u^2v^2 \rangle)$, and

(2) either u_1 or $(v^{-1})_1$ emanates from the basepoint of $\Gamma_X(\langle u^2v^2 \rangle)$,

then $\overline{uv}$ appears in $\Gamma_X(\langle \overline{u}^2\overline{v}^2 \rangle)$.

Proof. Observe the graph Γ, which is obtained by attaching a path labeled by w to the basepoint of $\Gamma_X(\langle u^2v^2 \rangle)$ and moving the basepoint to the origin of the w-path:



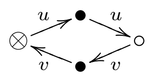
The graph Γ folds into $\Gamma_X(\pi_1^X(\Gamma)) = \Gamma_X(\langle \overline{u}^2\overline{v}^2 \rangle)$, since if satisfies the conditions of Lemma 2.1: the only vertex that needs checking is the gluing place, and there the conditions hold by assumption *(2)* and the fact that $w^{-1} \perp u, v^{-1}$ (as $\overline{u}, \overline{v}$ are reduced). Finally, since uv appears in $\Gamma_X(\langle u^2v^2 \rangle)$, $\overline{uv} = wuvw^{-1}$ appears in Γ, and thus also in its folding $\Gamma_X(\langle \overline{u}^2\overline{v}^2 \rangle)$. ◻

Lemma 4.3. *If $\{u, v\}$ is a CR basis of $\mathbf{F}_2$ then*

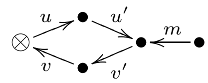
(1) uv appears in $\Gamma_X(\langle u^2v^2 \rangle)$, and

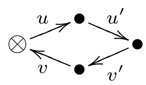
(2) u_1 or $(v^{-1})_1$ emanates from the basepoint of $\Gamma_X(\langle u^2v^2 \rangle)$.

Proof. If $|u| + |v| = 2$ then the claims hold, so assume that $|u| + |v| \geq 3$. Since $\Gamma_X\left(\left\langle u^2v^2\right\rangle\right) = \Gamma_X\left(\left\langle v^{-2}u^{-2}\right\rangle\right)$ and $\Gamma_X\left(\left\langle u^2v^2, uv\right\rangle\right) = \Gamma_X\left(\left\langle v^{-2}u^{-2}, v^{-1}u^{-1}\right\rangle\right)$, one can look at $\left\{v^{-1}, u^{-1}\right\}$ instead of $\{u, v\}$ (this also does not affect assertion *(2)*), and thus it is enough to handle the cases where $|u| < |v|$.

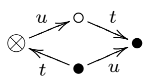
Observe the graph $\Gamma =$ 

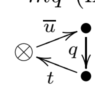
, which obviously satisfies $\pi_1^X(\Gamma) = \left\langle u^2v^2\right\rangle$. At the black vertices there can be no folding, as $u^{-1} \perp u$ follows from u being CR, and likewise for v. In what follows we will continue to mark by $\bullet$ vertices at which we already know that no folding can occur, and by $\circ$ vertices at which we do not know this.

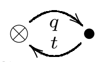
Assume first that u^{-1} is not a prefix of v, and m is the maximal common prefix of u^{-1} and v. Writing $u = u'm^{-1}$ and $v = mv'$, Γ folds into 

. After trimming one obtains $\Gamma' =$ 

, which satisfies the conditions of Lemma 2.1: $u^{-1} \perp u'$ since u is CR and u' is a prefix of u, and likewise for v and v'^{-1}; $u'^{-1} \perp v'$ by the maximality of m. Therefore, Γ' folds into $\Gamma_X\left(\left\langle u^2v^2\right\rangle\right)$. Since uv appears in Γ', and both u_1 and $\left(v^{-1}\right)_1$ leave its basepoint, the same holds after any foldings, and in particular in $\Gamma_X\left(\left\langle u^2v^2\right\rangle\right)$.

Assume now that u^{-1} is a prefix of v and write $v = u^{-1}t$. Now Γ folds and trims into 

, as $u \perp t$ and $t^{-1} \perp u^{-1}$ follow from $v = u^{-1}t$ being CR. Let m be the maximal common prefix of u^{-1} and tu^{-1}, and write $u = \overline{u}m^{-1}$, $tu^{-1} = mq$ (note that $\left|tu^{-1}\right| > \left|u^{-1}\right| \geq |m|$). The last graph then folds and trims into $\Gamma' =$ 

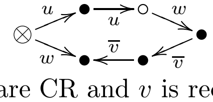
(with $\overline{u}$ possibly empty, in which case $\Gamma' =$ 

). This graph satisfies the conditions of Lemma 2.1: $q^{-1} \perp t$ since $tu^{-1} = mq$ is CR, being a cyclic rotation of v, and if $\overline{u}$ is not empty then $\overline{u}^{-1} \perp q$ by maximality of m. Since $uv = t$ appears in Γ' and $\left(t^{-1}\right)_1 = \left(v^{-1}\right)_1$ leaves its basepoint, the same holds for $\Gamma_X\left(\left\langle u^2v^2\right\rangle\right)$, which is obtained from it by foldings. $\square$

Lemma 4.4. *If $\{u, v\}$ is a basis of $\mathbf{F}_2$ with u or v CR then*

(1) uv appears in $\Gamma_X\left(\left\langle u^2v^2\right\rangle\right)$, and

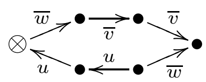
(2) u_1 or $\left(v^{-1}\right)_1$ emanates from the basepoint of $\Gamma_X\left(\left\langle u^2v^2\right\rangle\right)$.

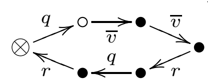
Proof. If both u and v are CR then we are done by Lemma 4.3. Again, by replacing u and v with v^{-1} and u^{-1} respectively we can assume that u is CR and v is not (here u is not necessarily shorter). Writing $v = w\overline{v}w^{-1}$ with $\overline{v}$ CR (and $w \neq 1$), w is a prefix of some power of u or u^{-1} by Lemma 3.1. The graph formed by a single u^2v^2-loop folds and trims into $\Gamma =$ 

, where at all the black vertices there can be no folding since u and $\overline{v}$ are CR and v is reduced.

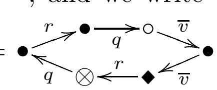
If w is a prefix of a (positive) power of u then at $\circ$ there is no folding as well since u is CR, so that $\Gamma_X\left(\langle u^2v^2\rangle\right)$ is obtained from Γ by foldings. Therefore to establish that uv appears in $\Gamma_X\left(\langle u^2v^2\rangle\right)$ it is enough to show that it appears in Γ. This is not obvious in first sight, but it is true: w is a prefix of a positive power of u, so that uw is a prefix of u^2w, hence $uv = uw\overline{v}w^{-1}$ indeed appears in Γ. Finally, both u_1 and $\left(v^{-1}\right)_1 = w_1$ leave the basepoint of Γ and thus also of $\Gamma_X\left(\langle u^2v^2\rangle\right)$.

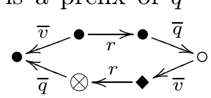
We assume now that w is a prefix of some power of u^{-1}, and observe six cases.

Case (i): $2|u| \le |w|$, so that $w = u^{-2}\overline{w}$ with $\overline{w}$ possibly empty. In this case Γ folds and trims into $\Gamma' =$ , which satisfies Lemma 2.1 (even if $\overline{w} = 1$). Now $uv = u^{-1}\overline{w}\overline{v}\overline{w}^{-1}u^2$ appears in Γ': $\overline{v}\overline{w}^{-1}u^2$ is a suffix of Γ' oriented clockwise, and $u^{-1}\overline{w}$ is a prefix of Γ' oriented counterclockwise since $\overline{w}$ is a prefix of $u^{-1}\overline{w}$. In addition, $\left(v^{-1}\right)_1 = w_1 = \left(u^{-1}\right)_1$ leaves $\otimes$.

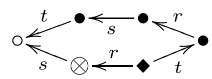
Case (ii): $|u| < |w| < 2|u|$, so that we can write $u = qr$ and $w = r^{-1}q^{-1}r^{-1}$ with $q, r \ne 1$. Now Γ folds and trims into $\Gamma' =$ , and no folding can occur at the black vertices. If at $\circ$ there is no folding as well, then $uv = r^{-1}\overline{v}rqr$ appears in Γ' and $\left(v^{-1}\right)_1 = w_1 = \left(r^{-1}\right)_1$ leaves $\otimes$, yielding the same for $\Gamma_X\left(\langle u^2v^2\rangle\right)$.
Assume now that there is folding at $\circ$, so that q^{-1} and $\overline{v}^2$ have a common prefix. If this prefix is shorter than $|\overline{v}|$ than the $\overline{v}rqr$ part in Γ' survives in $\Gamma_X\left(\langle u^2v^2\rangle\right)$, and thus $uv = r^{-1}\overline{v}rqr$ still appears in it. Otherwise, $\overline{v}$ is a prefix of q^{-1}, so that $r^{-1}\overline{v}$ is a prefix of Γ' oriented CCW, and rqr is a suffix of Γ' oriented CW, so that uv appears already in the lower half of Γ'. Finally, this half survives in $\Gamma_X\left(\langle u^2v^2\rangle\right)$ since q^{-1} cannot overlap with r, since $u = qr$ is monotone by Proposition 3.3. In both cases $\left(v^{-1}\right)_1 = \left(r^{-1}\right)_1$ still leaves $\otimes$.

Case (iii): $w = u^{-1}$. The reasoning here is as in the previous case with $r = 1$.

In cases ***(iv) – (vi)*** w is a proper prefix of u^{-1}, and we write $u = qr$ and $w = r^{-1}$ (with $r, q \ne 1$). Here Γ folds and trims into $\Gamma' =$ , with folding possible only at $\circ$, and the folding cannot reach past $\blacklozenge$ due to the monotonicity of $u = qr$. This already shows that $\left(v^{-1}\right)_1 = \left(r^{-1}\right)_1$ must leave the basepoint of the final Stallings graph $\Gamma_X\left(\langle u^2v^2\rangle\right)$. It is left to show that the folding and trimming at $\circ$ does not prevent $uv = q\overline{v}r$ from appearing in $\Gamma_X\left(\langle u^2v^2\rangle\right)$. If the lower half of Γ' survives the folding and trimming then uv certainly appears in it. We assume therefore that there is folding at $\circ$, and that it encompasses either all of $\overline{v}$ to the right of $\circ$ or all of rq to the left of it (i.e. it reaches the lower half of Γ').

Case (iv): $|\overline{v}| \le |q|$. By our assumption, $\overline{v}$ is a prefix of q^{-1}, so $q = \overline{q}\overline{v}^{-1}$ ($\overline{q}$ may be empty). Γ' then folds and trims into $\Gamma'' =$ . Now $uv = q\overline{v}r = \overline{q}r$ and since the folding from $\circ$ downward must stop at $\blacklozenge$ (or earlier), the $\bullet \xleftarrow{\overline{q}} \otimes \xleftarrow{r} \blacklozenge$ part survives in $\Gamma_X\left(\langle u^2v^2\rangle\right)$ (since $|\overline{v}| < |\overline{q}^{-1}r^{-1}\overline{v}|$) and we are done.

Case (v): $|q| < |\overline{v}| \le |rq|$. Now we can assume that $\overline{v}$ is a prefix of $q^{-1}r^{-1}$, so that $r = st$ and $\overline{v} = q^{-1}t^{-1}$ (possibly with $s = 1$). In this case $uv = q\overline{v}r = t^{-1}r$ already appears in the $\otimes \xleftarrow{r} \blacklozenge$ part of Γ', which always survives due to monotonicity.

Case (vi): $|rq| < |\overline{v}|$. Now we can assume that $q^{-1}r^{-1}$ is a prefix of $\overline{v}$. Therefore, $uv = q\overline{v}r$ is a suffix of $\overline{v}r$, and thus appears in the $\otimes \xleftarrow{r} \blacklozenge \xleftarrow{\overline{v}} \bullet$ part in Γ'. If $\overline{v}$ is not a prefix of $q^{-1}r^{-1}q^{-1}$ then the folding from $\circ$ downward stops before reaching this part, and we are done. We thus add the assumption that $\overline{v}$ is a prefix of $q^{-1}r^{-1}q^{-1}$. Since $|rq| < |\overline{v}|$ we can write $q = st$ so that $\overline{v} = q^{-1}r^{-1}t^{-1} = t^{-1}s^{-1}r^{-1}t^{-1}$. Now Γ' folds and trims into $\Gamma'' =$ , and $uv = r^{-1}t^{-1}r$ appears in $\otimes \xleftarrow{r} \blacklozenge \xrightarrow{t} \bullet$, which survives any further folding since $|s| < \left|t^{-1}s^{-1}r^{-1}\right|$. □

5 Epilogue

While the original conjecture [MVW07, §5(1)] fails, it is plausible that some modification of it holds. One possible option is the following:

Conjecture 5.1. *Let $H \le J$ be subgroups of the free group $\mathbf{F}$. Then $H \le_{alg} J$ iff $H \le_{\vec{X}} J$ for every free extension $\mathbf{F}'$ of $\mathbf{F}$, and every basis X of $\mathbf{F}'$.*

Since the relation $H \le_{alg} J$ does not depend on the ambient group, one direction holds as before. But in contrast with the original conjecture, the example in Section 4 is no longer a counterexample: let $\mathbf{F} = \mathbf{F}(a,b)$, $H = \langle a^2b^2 \rangle$ and $J = \langle ab, a^2b^2 \rangle$. For $\mathbf{F}' = \mathbf{F}(a,b,c)$ and $X = \{a, cb^{-1}, cbc^{-1}\}$, H does not X-cover J: denote $x = a$, $y = cb^{-1}$ and $z = cbc^{-1}$. Then written in this basis, $H = \langle x^2y^{-1}z^2y \rangle$ and $J = \langle x^2y^{-1}z^2y, xy^{-1}zy \rangle$. By Lemma 2.3, $H \le_{\vec{X}} J$ iff $xy^{-1}zy$ appears in $\Gamma_{\{x,y,z\}}\left(\langle x^2y^{-1}z^2y \rangle\right)$, which is not the case.

Another plausible option is that the original conjecture from [MVW07, §5(1)] holds for free groups of rank three or more, as it is clear that the counterexample exploits many idiosyncrasies of $\mathbf{F}_2$. If this is true, then Conjecture 5.1 follows as well.

References

[CMZ81] M. Cohen, W. Metzler, and A. Zimmermann, *What does a basis of $F(a,b)$ look like?*, Mathematische Annalen **257** (1981), no. 4, 435–445.

[Coh72] H. Cohn, *Markoff forms and primitive words*, Mathematische Annalen **196** (1972), no. 1, 8–22.

[KM02] I. Kapovich and A. Myasnikov, *Stallings foldings and subgroups of free groups*, Journal of Algebra **248** (2002), no. 2, 608–668.

[MVW07] A. Miasnikov, E. Ventura, and P. Weil, *Algebraic extensions in free groups*, Geometric group theory (G.N. Arzhantseva, L. Bartholdi, J. Burillo, and E. Ventura, eds.), Trends Math., Birkhauser, 2007, pp. 225–253.

[Nie17] J. Nielsen, *Die isomorphismen der allgemeinen, unendlichen gruppe mit zwei erzeugenden*, Mathematische Annalen **78** (1917), no. 1, 385–397.

[OZ81] R. P. Osborne and H. Zieschang, *Primitives in the free group on two generators*, Inventiones Mathematicae **63** (1981), no. 1, 17–24.

[PP12] D. Puder and O. Parzanchevski, *Measure preserving words are primitive*, Arxiv preprint arXiv:1202.3269 (2012).

[Pud11] D. Puder, *Primitive words, free factors and measure preservation*, Arxiv preprint arXiv:1104.3991 (2011).

[Sta83] J. R. Stallings, *Topology of finite graphs*, Inventiones mathematicae **71** (1983), no. 3, 551–565.

[Tak51] M. Takahasi, *Note on chain conditions in free groups*, Osaka Math. J **3** (1951), no. 2, 221–225.